UNIT III TELEMEDICAL STANDARDS

Data Security and Standards: Encryption, Cryptography, Mechanisms of encryption, phases of Encryption. Protocols: TCP/IP, ISO-OSI, Standards to followed DICOM, HL7, H.320 series Video Conferencing, Security and confidentiality of medical records, Cyber laws related to telemedicine

1. Data Security and Standards

1.1 Standards

- Defn: a common language which has common definitions, terms of reference, rules of procedures, terminology and many other factors
- Types of standards

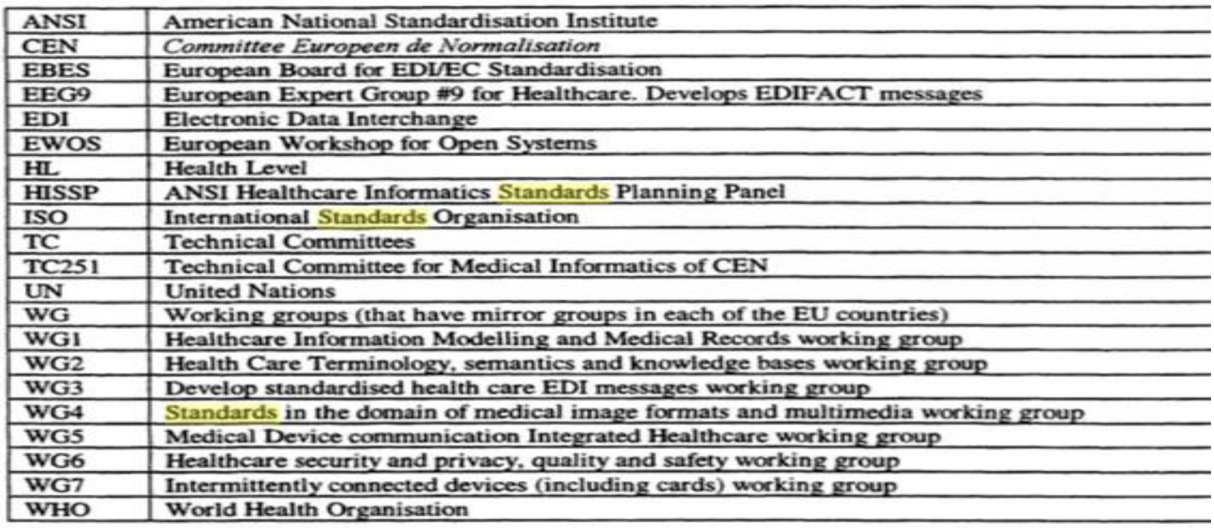
1. *De facto standards*

- A **format, language, or protocol** that has become a standard because
  - it is approved by a standards organization
  - Reached and recognized by the industry/market in a given period of time.
  - E.g., The QWERTY system for keyboards accepted but other types like AZERTY (French-speaking countries across Europe and Africa)

2. *Consensus standards*

- Consensus standards are *developed by* ***ad hoc committees*** *and* ***expert bodies*** *those are interested in* ***participating in the development and/or use of the standards*** *with a legal/professional mandate.*
- E.g., X-25 telecommunications protocol, decided and published by CCITT(now ITU-T)[International Telegraph and Telephone Consultative Committee]

- Main standardization bodies are

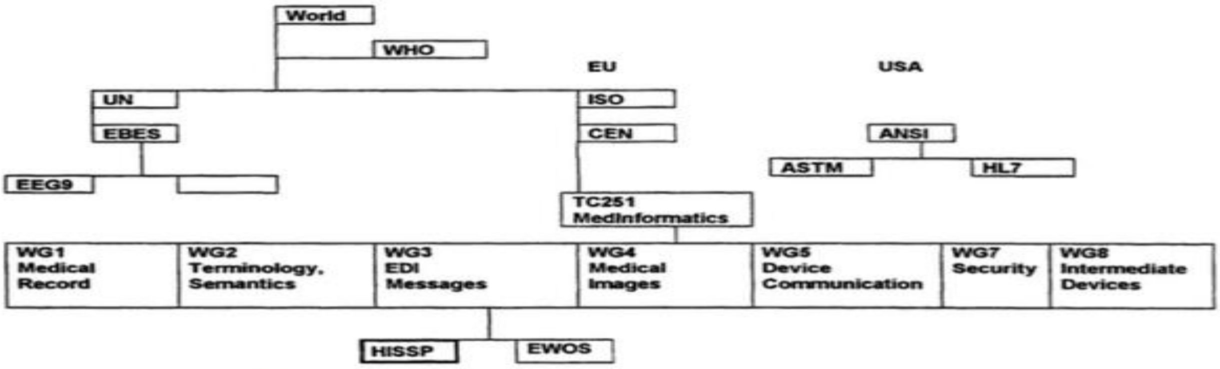


ANSI	American National Standardisation Institute
CEN	*Committee Europeen de Normalisation*
EBES	European Board for EDI/EC Standardisation
EEG9	European Expert Group #9 for Healthcare. Develops EDIFACT messages
EDI	Electronic Data Interchange
EWOS	European Workshop for Open Systems
HL	Health Level
HISSP	ANSI Healthcare Informatics Standards Planning Panel
ISO	International Standards Organisation
TC	Technical Committees
TC251	Technical Committee for Medical Informatics of CEN
UN	United Nations
WG	Working groups (that have mirror groups in each of the EU countries)
WG1	Healthcare Information Modelling and Medical Records working group
WG2	Health Care Terminology, semantics and knowledge bases working group
WG3	Develop standardised health care EDI messages working group
WG4	Standards in the domain of medical image formats and multimedia working group
WG5	Medical Device communication Integrated Healthcare working group
WG6	Healthcare security and privacy, quality and safety working group
WG7	Intermittently connected devices (including cards) working group
WHO	World Health Organisation

1.2 Telemedical Standards

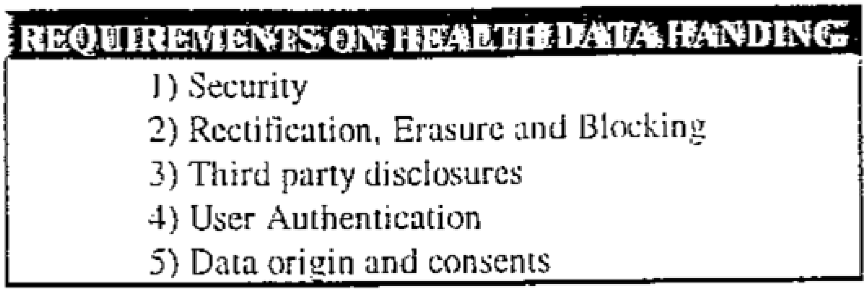
- Defn: process that **insure effective and safe delivery of quality healthcare**
- They will allow for a **fast development of solutions and applications**

- Standards should be adopted to **data codes, formats, messages , health records, signals, medical images , medical devices and data protection** => provides **interoperability** of health information systems, **compatibility** of data and the **practical use** of it
- Pictorial representation of **International standards organization and their geographical coverage**



International standards organisations and their geographical coverage.

- Standards in **Health Data Handling** are regulated by the standard body of Informatics that classify information in terms of **REQUIREMENTS** on the 5 following points



REQUIREMENTS ON HEALTH DATA HANDING

1) Security
2) Rectification, Erasure and Blocking
3) Third party disclosures
4) User Authentication
5) Data origin and consents

Health Information System requirements

- ✓ Rectification, erasure and blocking: a digital signature for any modification, date and time of all messages, backups on a non-erasable recording device must be certified by a third party.

- ✓ Third party disclosure
  - rectify, erase or block data third party must notify
  - third party disclosure register is kept as apart of the patient record
- ✓ User Authentication: user should be authorized and authenticated

1.3 Security

- Data security is a ***set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure.***
- Data security can be ***applied using a range of techniques and technologies*** that limit access to unauthorized or malicious users or processes.
- **Mechanism of security :** They are based on triplet

a. **Confidentiality:** property which ***assures only authorized users can have access to the system***. Violations can be found in
   - Unauthorized access
   - Falsifying user identity
   - Making unauthorized copies
   - Intercepting messages

b. **Integrity :** is the quality which ***insures that information is only modified by its usual users***

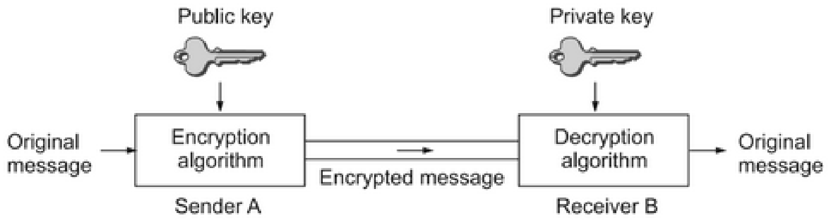
c. **Disposal or Availability:** is the ***ability of an information system is used by authorized users.*** Violation poses serious doubts on data integrity, secure medical practice

1.4 Cryptography , Encryption

- ➢ Cryptographic procedures can basically be of two types :
  1. **On person to person basis** (private key cryptography)
     - ✓ An individual user generate a key pair and protect the private key with a password
     - ✓ Key generation is done with the program PGP (Pretty Good privacy) based on RSA algorithm /Hash Algorithm.
     - ✓ Hash Algorithm : Message Digest(MD2, MD4, MD5) /SHA(Secure Hash Algorithm
  2. **On world basis**
     - ✓ A Trusted third party authentication of key management is required
     - ✓ They generate the key pair
- ➢ Encryption
  - ✓ is the process of ***translating plain text data (plaintext) into unreadable format called cipher text.***
  - ✓ is a scheme ***which scrambles contents of a message using mathematical schemes and algorithms***
- ➢ Decryption
  - ✓ is the process of ***converting ciphertext back to plaintext***
  - ✓ Done in conjunction with the use of secret keys=> those who poses cryptographic keys (long random number) can decrypt the message.
- ➢ Cryptographic keys are classified as

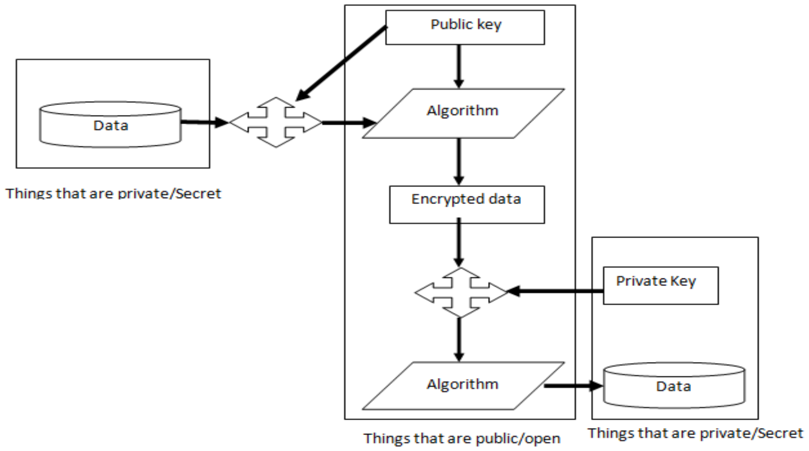
  1. Public key cryptography/asymmetric cryptography
  - ✓ uses two mathematically related, but not identical, ***pair keys - a public key and a private key(each person gets a pair of keys)***
  - ✓ Each public key is published, and the corresponding private key is kept secret.

- ✓ Data encrypted with a public key can be decrypted only with the corresponding private key.
- ✓ E.g., When A wants to send B a secure message, he encrypts using B's public key. When B gets the message, he decrypts it using his private key
- ✓ Pictorial representation of Public key encryption



Public key encryption

- ✓ Public key for encryption is used to generate a private key for decryption=>different individuals will have a pair of different keys
- ✓ Eliminates the ***risk of secret key being stolen***=> only public key is sent through the network.
- ✓ Algorithms used are
  - RSA (*Rivest–Shamir–Adleman)*algorithm
  - Hash Algorithm used in digital signatures


Public key
Data
Algorithm
Things that are private/Secret
Encrypted data
Private Key
Algorithm
Data
Things that are public/open
Things that are private/Secret

2. Private key/secret key Cryptography/Symmetric key Encryption

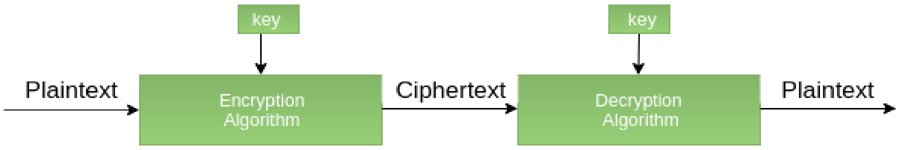
- ✓ is the form of encryption where **only a single private key can encrypt and decrypt information**
- ✓ Requires a **secure channel be used to exchange the key** between the sender and receiver
- ✓ The **strength of symmetric key cryptography depends upon the number of key bits**
- ✓ **fast process** since it uses a single key

ciphertext = encrypt(plaintext, key)

plaintext = decrypt(ciphertext, key)

✓ Algorithms are

- DES(Data Encryption Standard)
- IDEA(International data encryption algorithm)=128 bit key



➢ In telemedicine, **encryption can be done on voice, data and video for both store and forward and real-time communications sessions.**

➢ DES(data Encryption Standards) is defined in IT acts of respective countries can be applied to telemedicine

➢ The Encryption standards are

a. Triple DES(enhancement of DES)

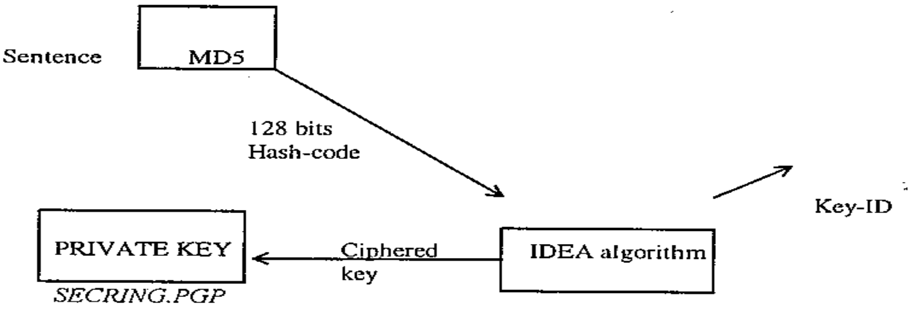
b. Encrypt decrypt encrypt

c. Cipher Block Chaining(CBC)

d. Advanced Encryption Standard(AES)

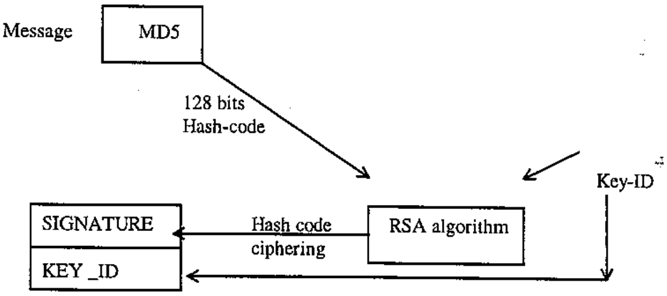
1.5 Phases of Encryption

➢ *PGP –Private key generation*



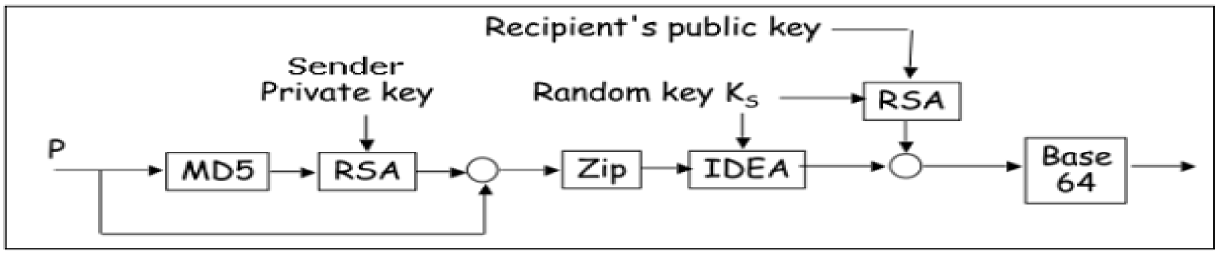
Private key generation

➢ *PGP Digital Signature Generation-private key involved*



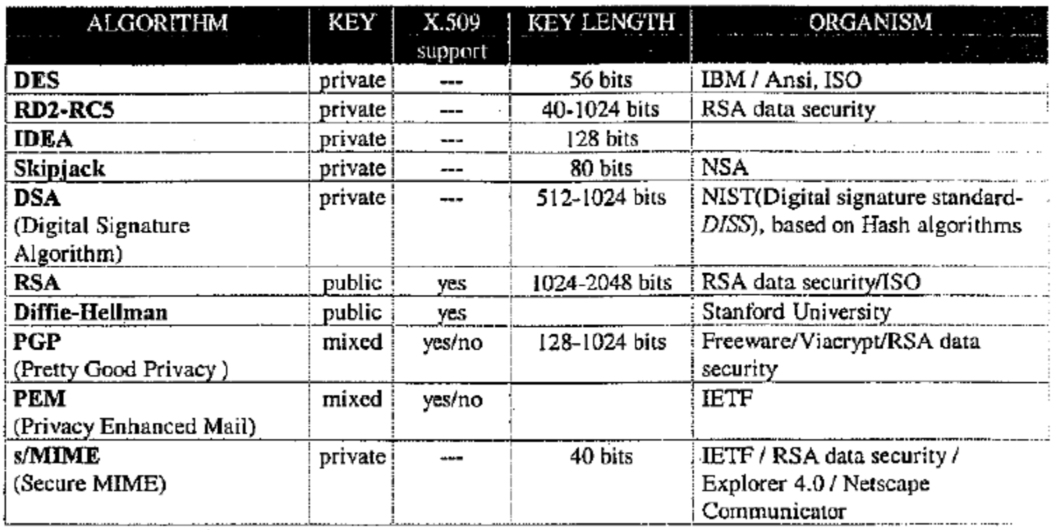
Digital signature generation

➢ *Compression and ciphering of PGP*



- Hash of the message is calculated. (MD5 algorithm)
- Resultant 128 bit hash is signed using the private key of the sender (RSA Algorithm).
- The digital signature is concatenated to message, and the result is compressed.
- A 128-bit symmetric key, K_S is generated and used to encrypt the compressed message with IDEA.
- K_S is encrypted using the public key of the recipient using RSA algorithm and the result is appended to the encrypted message.

➢ Some of Encryption algorithm



ALGORITHM	KEY	X.509 support	KEY LENGTH	ORGANISM
DES	private	---	56 bits	IBM / Ansi, ISO
RD2-RC5	private	---	40-1024 bits	RSA data security
IDEA	private	---	128 bits	
Skipjack	private	---	80 bits	NSA
DSA (Digital Signature Algorithm)	private	---	512-1024 bits	NIST(Digital signature standard-*DISS*), based on Hash algorithms
RSA	public	yes	1024-2048 bits	RSA data security/ISO
Diffie-Hellman	public	yes		Stanford University
PGP (Pretty Good Privacy)	mixed	yes/no	128-1024 bits	Freeware/Viacrypt/RSA data security
PEM (Privacy Enhanced Mail)	mixed	yes/no		IETF
s/MIME (Secure MIME)	private	---	40 bits	IETF / RSA data security / Explorer 4.0 / Netscape Communicator

2. Protocols

➢ A protocol is a **set of rules** that govern how systems communicate

➢ These rules **must be followed by each machine** involved in the communication.

➢ These protocols **describe the movement of data** between the source and destination or the internet

Or

➢ Is a formal, well-defined set of rules for exchange information between computer programs

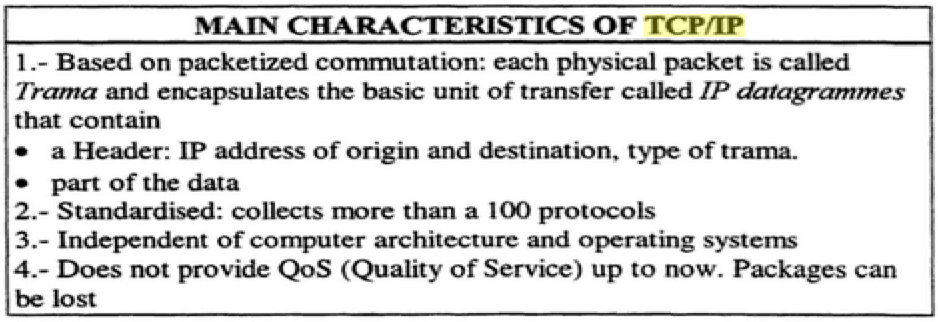
2.1 TCP/IP

- was developed by Department of **Defence's Advanced Project Research Agency** (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- TCP/IP means **Transmission Control Protocol and Internet Protocol**.
- It is the network model used in the **current Internet architecture**.
- TCP/IP is a two-layer program.
  - ✓ **The higher layer, Transmission Control Protocol (TCP)**, assembles the message or file into smaller packets that are transmitted over the Internet and reassembles the received packets into the original message.
  - ✓ **The lower layer, Internet Protocol (IP)**, handles the address part of each packet so that it gets to the right destination.
- The TCP/IP model consists of five layers: **the application layer, transport layer, network layer, data link layer and physical layer**.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

<table>
<tr><th colspan="7">Levels of conformance between Internet and ISO model</th></tr>
<tr><th>TCP/IP
(Internet)</th><th colspan="5">Protocols & Networks</th><th>ISO/OSI</th></tr>
<tr><td rowspan="3">Application Layer</td><td rowspan="3">Software
applications</td><td rowspan="3" colspan="3">Telnet
FTP
SMTP</td><td rowspan="3">HTTP
Java
SNMP</td><td>Application Layer</td></tr>
<tr><td>Presentation Layer</td></tr>
<tr><td>Session Layer</td></tr>
<tr><td>Transport Layer</td><td colspan="2">TCP</td><td colspan="3">UDP</td><td>Transport Layer</td></tr>
<tr><td>Internet Layer</td><td colspan="5">IP</td><td>Network Layer</td></tr>
<tr><td rowspan="2">Network Interface</td><td colspan="2">ARP/RARP</td><td>X.25</td><td colspan="2">SLIP… etc.,</td><td>Link Layer</td></tr>
<tr><td colspan="5">Ethernet… etc.,</td><td>Physical Layer</td></tr>
</table>

- Main characteristics of TCP/IP protocol



MAIN CHARACTERISTICS OF TCP/IP

1.- Based on packetized commutation: each physical packet is called *Trama* and encapsulates the basic unit of transfer called *IP datagrammes* that contain

- a Header: IP address of origin and destination, type of trama.
- part of the data

2.- Standardised: collects more than a 100 protocols

3.- Independent of computer architecture and operating systems

4.- Does not provide QoS (Quality of Service) up to now. Packages can be lost

- **Different Layers of TCP/IP Reference Model**

  1. **Network Interface layer**

  - ▪ The lowest layer of the TCP/IP model.
  - ▪ Is the **combination of the Physical layer and Data Link layer** defined in the OSI reference model

- It defines **how the data should be sent between two devices physically through the network**.
- The functions of this layer is **encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses**.
- technologies used can be LAN-based (e.g. Ethernet) or WAN-based (e.g. ISDN)
- Varies from host to host and network to network.

2. Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The various functions performed by the Internet Layer are
  a) Delivering IP packets
  b) Performing routing
  c) Avoiding congestion
- Different types of protocol used in this layer are
  a) IP Protocol
  b) ARP(**Address Resolution Protocol**) protocol
  c) **ICMP(**Internet Control Message Protocol) **Protocol**

3. Transport Layer

- is responsible for the **reliability, flow control(stop and wait, sliding window), and correction of data** which is being sent over the network.
- two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.
- Functions such as **multiplexing, segmenting or splitting on the data** and **adds header** information to the data and **breaks the message** (data segments) into small units so that they are handled more efficiently by the network layer.
- Transport layer also **arrange the packets to be sent, in sequence.**

4. Application Layer

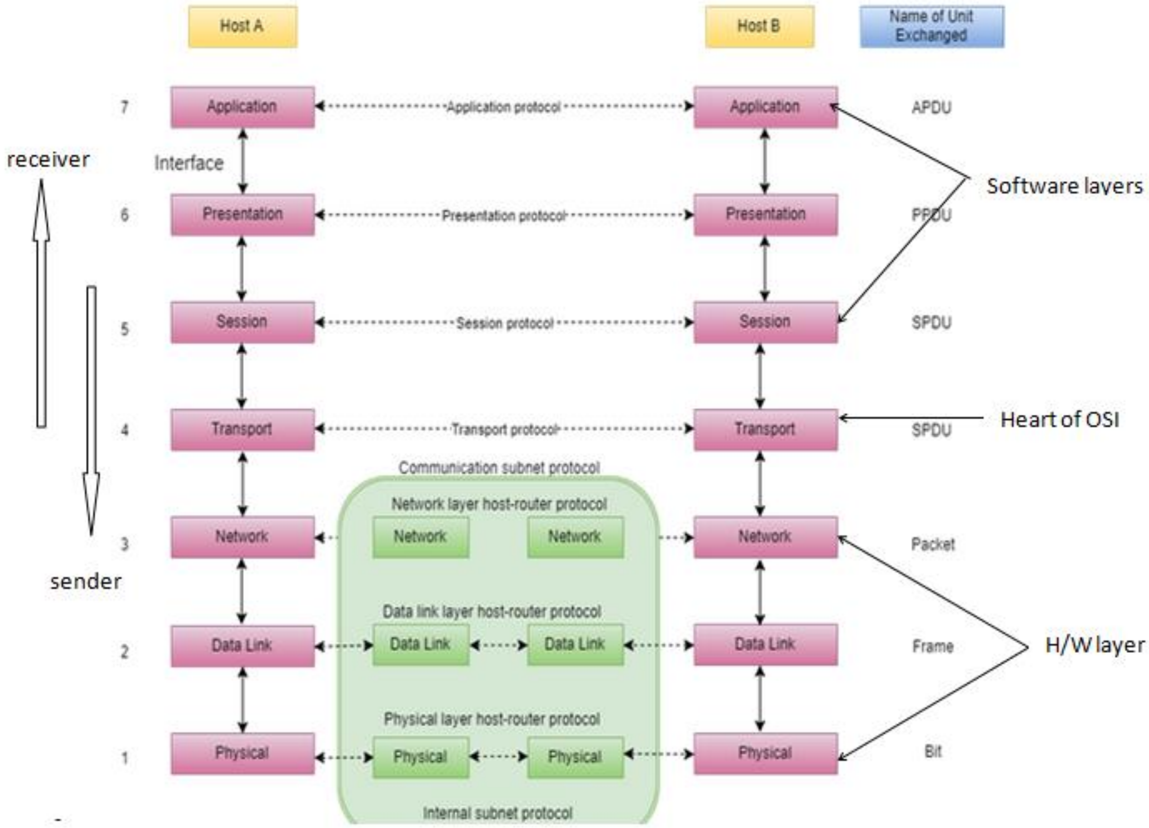
- is the **topmost layer** in the TCP/IP model.
- includes the OSI **Presentation Layer and Session Layer**
- responsible for **handling high-level protocols, issues of representation(syntax and semantics)**
- allows the **user to interact with the application**
- Main protocols used in the application layer
  HTTP, SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), TELNET (Terminal Network), FTP (File Transfer Protocol)

- **Merits of TCP/IP**

  - It is **interoperable**, i.e., it **allows cross-platform communications** among heterogeneous networks.
  - it is an **open protocol suite**
  - It is a **scalable, client-server architecture**. This allows networks to be added without disrupting the current services.
  - it **assigns an IP address to each computer** on the network, thus making each device to be identifiable over the network. It assigns each site a domain name. It provides name and address resolution services.
  - Supports a number of routing protocols.
  - It operates/works independently of the operating system.
- **Demerits of TCP/IP**
  - It is not **generic in nature**. So, it fails to represent any protocol stack other than the TCP/IP suite. For example, it cannot describe the Bluetooth connection
  - It was originally **designed and implemented for wide area networks**. It is **not optimized for small networks like LAN (local area network) and PAN (personal area network).**
  - the transport layer **does not guarantee delivery of packets**
  - It has not **clearly separated its services, interfaces and protocols**.

2.2 ISO/OSI

- OSI stands for **Open Systems Interconnection**.
- It has been developed by ISO – '**International Organization of Standardization**', in the year 1984.
- The OSI model is a layered model that explains **how information travels from two different applications running on two different networked computers.**
- Fundamentally, the OSI model **regulates the steps to transfer data over a transmission channel between two network devices**
- The OSI (Open System Interconnection) Reference Model is the comprehensive **set of standards and rules** for hardware manufacturers and software developers to build the networking components and software applications which work in dissimilar environments.
- It is seven **layer architecture** with each layer having specific functionality to perform.
- All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
-



- Functions of OSI Layers

Group	Layer Number	Layer Name	Description
Top Layers	7	Application	Provide user interface to send and receive the data
	6	Presentation	Encrypt, format and compress the data for transmission
	5	Session	Initiate and terminate session with remote system
Bottom Layers	4	Transport	Break data stream in smaller segments and provide reliable and unreliable data delivery
	3	Network	Provide logical addressing
	2	Data Link	Prepare data for transmission
	1	Physical	Move data between devices

- OSI model is divided into two layers: upper layers and lower layers.
  - **upper layer :** deals with the **application related issues**, and is implemented only in the software.
  - **lower layer** : deals with the **data transport issues**.
  - The data link layer and the physical layer are implemented in hardware and software.

1. **Physical Layer**

- **Activates, maintains and deactivates** the physical connection between the devices.
- On sending computer, it converts digital signals received from the Data Link layer, into analog signals and loads them in physical media. On receiving computer, it picks analog signals from media and converts them in digital signals and transfers them to the Data Link layer for further processing.
- **Hub, Repeater, Modem, Cables** are Physical Layer devices

2. **Data Link Layer**

- responsible for the **error-free transfer of data frames from node-to-node delivery of data over the physical layer.**
- **Functions of Data-link layer**
  i. Handle errors by implementing an acknowledgement and retransmission scheme
  ii. Regulate the flow of control
  iii. Provide a well defined interface to the network layer
- It **receives the data from network layer and creates FRAMES , add physical address to these frames & pass them to physical layer**
- Switch & Bridge are Data Link Layer devices**.**
- has two sub-layers; MAC and LLC.

a. MAC(Medium Access Control)

- Establishes a link between the Logical Link Control layer and physical layer.
- Converts logical address into physical address
- It is used for transferring the packets over the network.

b. Logical Link Control(LLC)

- is responsible for **synchronizing frames, error checking, and flow control**.

3. **Network Layer**

- responsible for the **delivery of packets from source to destination**
- Takes care of **packet routing** i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP address are placed in the header by network layer.
- Protocol used in Network Layer is IPv6
- functions of the Network layer

a. **Internetworking:** logical connection between different types of networks.(main duty of network layer)

b. **Addressing:** adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

c. **Routing:** determines the best optimal path out of the multiple paths from source to the destination.

d. **Packetizing:** encapsulates the packets received from upper layer protocol and makes new packets.. This process is known as Packetizing. It is achieved by internet protocol (IP).

4. **Transport Layer**

- ensures that **messages are transmitted in the order** in which they are sent and there is **no duplication of data.**
- main responsibility of the transport layer is to **transfer the data completely**.
- receives the data from the upper layer and **converts them into smaller units known as <u>segments.</u>**
- Called as **end-to-end layer** as it provides a point-to-point connection between source and destination to deliver the data reliably.
- two protocols used in this layer are **Transmission Control Protocol, User Datagram Protocol**

At sender's side:

- ✓ receives the formatted data from the upper layers, performs **Segmentation** and implements **Flow & Error control** to ensure proper data transmission.
- ✓ adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.
  Note: destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

At receiver's side:

- ✓ Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application.
- ✓ It also performs sequencing and reassembling of the segmented data.

5. **Session Layer**

- **Sets up, coordinates and terminates conversations** between applications
- services include **authentication and reconnection** after an interruption
- determines how long a system will wait for another application to respond.
- protocols include X.225, AppleTalk and Zone Information Protocol (ZIP).

6. **Presentation Layer**

- Translates or formats data for the application layer based on the semantics or syntax that the application accepts.
- This layer handles the **encryption and decryption** that the application layer requires.

- Presentation layer is **also known as the syntax layer**.

7. **Application Layer**
   - serves as a window for users and application processes to access network service
   - handles issues such as network transparency, resource allocation, etc
   - provides the network services to the end-users

- **advantages**
  - It is a **generic model** and acts as a guidance tool to develop any network model.
  - has all **flexibility to adapt to many protocols**
  - It distinctly separates **services, interfaces, and protocols**. Hence, it is flexible in nature. Protocols in each layer can be replaced very conveniently depending upon the nature of the network.
  - supports both **connection-oriented services and connectionless services**
- **Disadvantages**
  - very complex to understand and manage
  - Less privacy and easy to access.
  - Due to the complexity of OSI model, the first implementations were pretty heavy and slow.

Difference between TCP/IP and ISO/OSI

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.

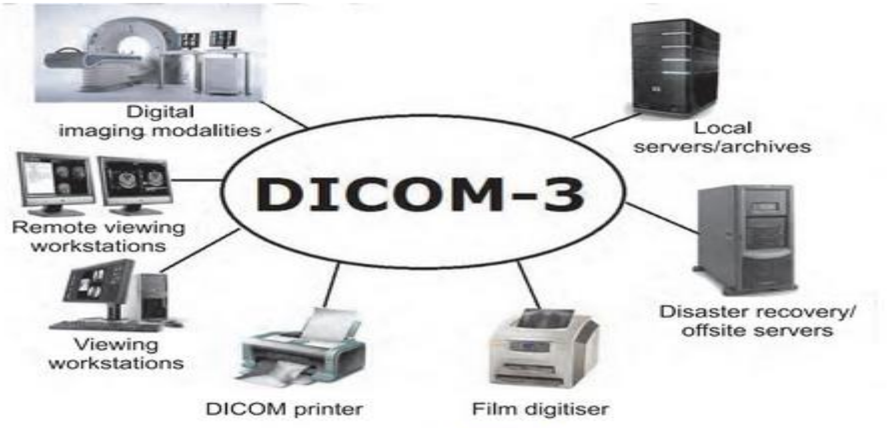
3. STANDARDS TO BE FOLLOWED

3.1 DICOM(Digital Image Communications in Medicine)

- is the **international standard** to transmit, store, retrieve, print, process, and display **medical imaging** information.
- Eg. DICOM transfers not only Radiology images, but also: - Cardiology (X-Ray Angio, US, NM) - Oncology (RT Portal images) - Dentistery (X-ray Intra-Oral) - Pathology, Endoscopy, Microscopy, Optalmology, etc.
- The DICOM standard covers both the **formats** to be used for storage of digital medical images and related digital data, and the **protocols** to be adopted to

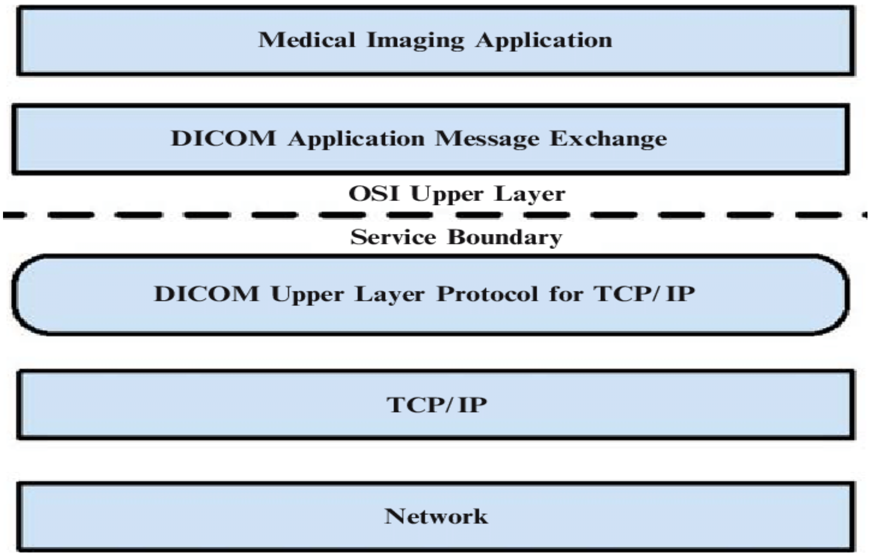
implement several communication services which are useful in the medical imaging workflow.

- Objectives of DICOM are
  - makes medical imaging information **interoperable**
  - **integrates** image-acquisition devices, PACS(Picture Archiving and Communication system), workstations, VNAs(A **Vendor Neutral Archive** (**VNA**) is a medical imaging technology in which images and documents (and potentially any file of clinical relevance) are stored (archived) in a standard format with a standard interface) and printers from different manufacturers
  - is actively developed and maintained to meet the **evolving** technologies and needs of medical imaging
- Developed by ACR(American College of Radiology) and NEMA(National Electrical Manufactures Association), **First successful DICOM Standard issued in 1993**
- Aim of DICOM standard is to have a **general standard that can be applied to all range of medical images in the healthcare field**
- Spectrum of applications of DICOM in integrating medical imaging devices in telemedicine

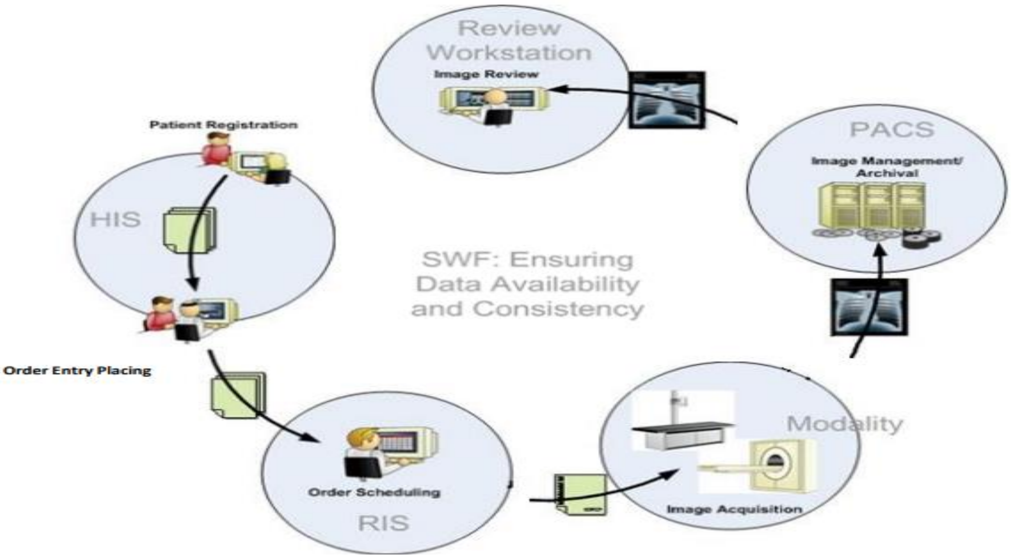

Digital imaging modalities
Local servers/archives
DICOM-3
Remote viewing workstations
Disaster recovery/ offsite servers
Viewing workstations
DICOM printer
Film digitiser

Spectrum of applications of DICOM standard

- **Basic Facts Of DICOM**
  - DICOM files typically have a **.dcm extension** and data contains both **patient data and the image/pixel data**. The patient data comes from the telemedicine application and image/pixel data created by the radiology medical imaging devices as DICOM data.
  - The DICOM protocol is a **binary Upper Level Protocol (ULP) over TCP/IP**. Well known ports used by DICOM are **104, 2761, 2762 and 11112**.
  - The DICOM Network Protocol architecture


Medical Imaging Application
DICOM Application Message Exchange
OSI Upper Layer
Service Boundary
DICOM Upper Layer Protocol for TCP/IP
TCP/IP
Network

- Work flow of DICOM



- File Format of DICOM
  - ➢ A DICOM file contains patient identification, site of origin, attributes of the image inclusive of pixel size, and the image itself.
  - ➢ File Format syntax

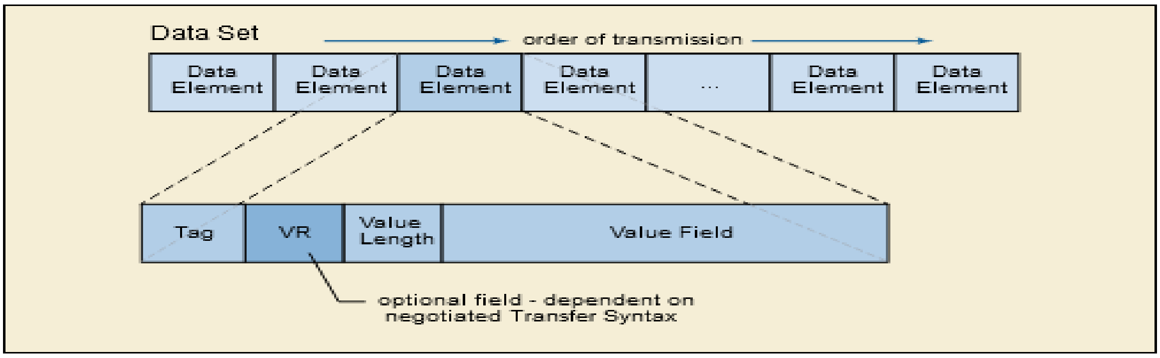
File Header		Data set/File Meta Elements						
File Preamble	DICOM Prefix	Data Element	Data Element	Data Element	Data Element	Data Element	………..	Data Element

- ➢ **File Header**
  - ✓ The header consists of a **128 byte File Preamble(meaning is preface)**, followed by a 4 byte DICOM prefix. The header may or may not be included in the file(set to 00H by default)
  - ✓ It facilitates **access to the images and other data in the DICOM file** by providing compatibility with a number of commonly used computer image file formats.

Preamble	Prefix
128 bytes =??? ???	4 bytes = 'D', 'I', 'C', 'M'

DICOM File Header

- **Data Set**
  - ✓ Data Set represents an instance of a real world Information Object.
  - ✓ A Data Set is constructed of Data Elements.
  - ✓ Data element is an atomic unit of data that has precise meaning or precise semantics



A DICOM *attribute* or *data element* is composed of:

- A *tag*, in the format of *group*, *element* (XXXX,XXXX) that identifies the element
- A *Value Representation* (VR) that describes the data type and format of the attribute's value
- A *value length* that defines the length of the attribute's value
- A *value field* containing the attribute's data

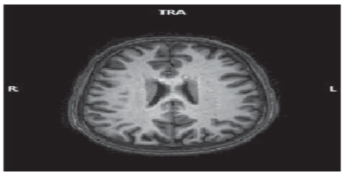
E.g.,

DICOM FILE (XX .dcm file)

Header

Field	Value
Format	'DICOM'
Width	256
Height	256
Bit Depth	12
Color type	'grayscale'
Manufacturer	'Philips medical systems'
Magnetic Field Strength	3 T
Series Number	501
Instance Number	1000
Patient Position	'HFS'
...	...

Image (256x 256 matrix)



- DICOM enables the **integration of scanners, servers, workstations, printers and network h/w from multiple manufactures into a PACS**

- A medical device supporting and implementing the DICOM standard is defined as a **DICOM-compliant device**. A "DICOM-compliant" device able to connect to the DICOM network exchange data with other nodes using the DICOM protocol.
- DICOM devices attached to a DICOM network are often referred to also as **DICOM nodes** or **DICOM peers**.
- DICOM supports **different storage media or across the network** to transfer the data (e.g., CD, MOD(Magneto optical drivers)).
- DICOM is based on **OSI reference model.**
- DICOM prefers **TCP/IP communication network** to transfer data from the data scanners, CT, MRI ,etc or between telemedicine systems.
- In DICOM, **grayscale** images are **16 bits per pixel**, **color** image are **24 bits per pixel** plus **8 bits per pixel for intensity** information
- **PACS (Picture Archiving and Communication System) normally composes of four basic elements**

  1) Medical imaging equipment like MRI, CT, X-ray, Ultrasound, and more.

  2) A **secure network for exchange** and distribution of patient examination data.

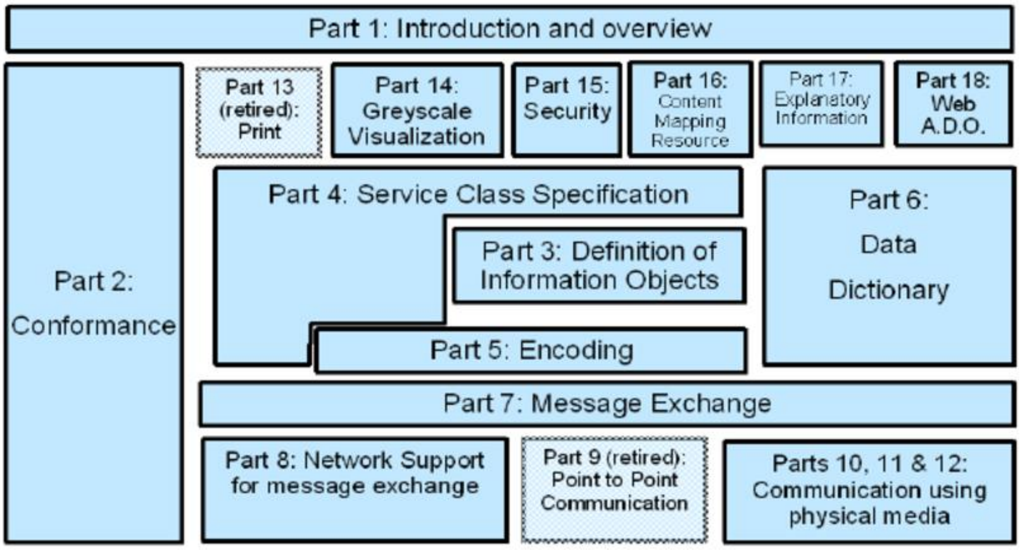
  3) DICOM workstations or mobile devices for **viewing, re-processing, and interpreting images.**

  4) It also archives and printers for **storage and retrieval of images** and related documentation and reports.

  ✓ PACS is a kind of the **integration of all above resources** in a healthcare organization to capture, store, view, and share the medical images internally or externally. And this makes it possible for remote diagnostic and interpretation of the images.
- DICOM Version 3.0 is composed of several hundreds of pages over sixteen separate parts. Each part of the standard focuses on a different aspect of the DICOM protocol:

  ✓ Part 1- Introduction and Overview
  ✓ Part 2 - Conformance
  ✓ Part 3: Information Object Definitions
  ✓ Part 4: Service Class Specifications
  ✓ Part 5: Data Structure and Semantics
  ✓ Part.6: Data Dictionary
  ✓ Part 7 : Message Exchange
  ✓ Part 8: Network Communication Support for Message Exchange
  ✓ Part 9: Retired (Formerly Point-to-Point Communication Support for Message Exchange)
  ✓ Part 10: Media Storage and File Format
  ✓ Part 11: Media Storage Application Profiles
  ✓ Part 12: Storage Functions and Media Formats for Data Interchange
  ✓ Part 13: Retired (Formerly Print Management Point-to-point Communication Support)
  ✓ Part 14: Grayscale Standard Display Function

- ✓ Part 15: Security and System Management Profiles
- ✓ Part 16: Content Mapping Resource
- ✓ Part 17: Explanatory Information
- ✓ Part 18: Web Access to DICOM Persistent Objects (WADO)
- ✓ Part 19: APPLICATION HOSTING
- ✓ Part 20: TRANSFORMATION OF DICOM TO AND FROM HL7 STANDARDS


Part 1: Introduction and overview
Part 2: Conformance
Part 13 (retired): Print
Part 14: Greyscale Visualization
Part 15: Security
Part 16: Content Mapping Resource
Part 17: Explanatory Information
Part 18: Web A.D.O.
Part 4: Service Class Specification
Part 3: Definition of Information Objects
Part 6: Data Dictionary
Part 5: Encoding
Part 7: Message Exchange
Part 8: Network Support for message exchange
Part 9 (retired): Point to Point Communication
Parts 10, 11 & 12: Communication using physical media

3.1.1 Basic Structures and Concepts in DICOM

- DICOM Objects are known as the **Information Object Definitions (IOD).**
- All real world data like patients, studies, medical devices, images, patient schedule list, a queue to be sent to a printer are objects with defined templates.
- A **DICOM modality** is a property/attribute of the DICOM data object, e.g. CT, MRI, X-rays etc. are the modalities
- DICOM applications provide the services required for the data exchange.
- DICOM Service Element (DIMSE) are used by Application Entities (AE).
- There are two types of DIMSE Services:
  i. Composite DIMSE-C

     The composite services were designed for compatibility with previous versions of the ACR-NEMA Standard. They were originally intended for storage (C-STORE), query (C-FIND), retrieval (C-GET), and transfer (C-MOVE) of images.

  ii. Normalized DIMSE-N.

     The normalized services were designed to provide broader information management functionality. The normalized services support the basic information management operations: create (N-CREATE), delete (N-DELETE), update (N-SET), and retrieve (N-GET). In addition, domain-specific operations (N-ACTION) such as “print a sheet of film” can be defined. A notification service (N-EVENT_NOTIFY) is also specified in the normalized group.

DICOM services

- DICOM consists of many different services, most of which involve transmission of data over a network
  a. **Store service:** is used to send images or other persistent objects (structured reports, etc.) to a PACS or workstation.
  b. **Storage Commitment**
  - ✓ is used to confirm that an image has been permanently stored by a device (either on redundant disks or on backup media, e.g . burnt to a CD).
  - ✓ The Service Class User (SCU - similar to a client), a modality or workstation, etc., uses the confirmation from the
  - ✓ Service Class Provider (SCP - similar to a server), an archive station for instance, to make sure that it is safe to delete the images locally
  c. **Query/Retrieve :** This enables a workstation to find lists of images or other such objects and then retrieve them from a PACS
  d. **Modality Worklist**
  - ✓ enables **imaging equipment (modalities) to query (using C-FIND) for details of patients**
  - ✓ The items in the worklist include details about the patient (patient ID, name, sex, and age), the type of procedure (equipment type, procedure description, procedure code) and the procedure order (referring physician, accession number, reason for exam).
  - ✓ E.g., An image acquisition device, such as a CT scanner, queries a service provider, such as a RIS, to get this information which is then presented to the system operator and is used by the imaging device to populate details in the image metadata.
  - ✓ Prior to the use of the DICOM modality worklist service, the scanner operator was required to manually enter all the relevant details. Manual entry is slower and introduces the risk of misspelled patient names, and other data entry errors.
  - ✓ avoiding the need to type such information multiple times (and the mistakes caused by retyping
  e. **Modality performed procedure step**
  enables the modality to send a report about a performed examination including data about the images acquired, beginning time, end time, and duration of a study, dose delivered, etc.
  f. **Print:** is used to send images to a DICOM printer, normally to print an "X-Ray" film.

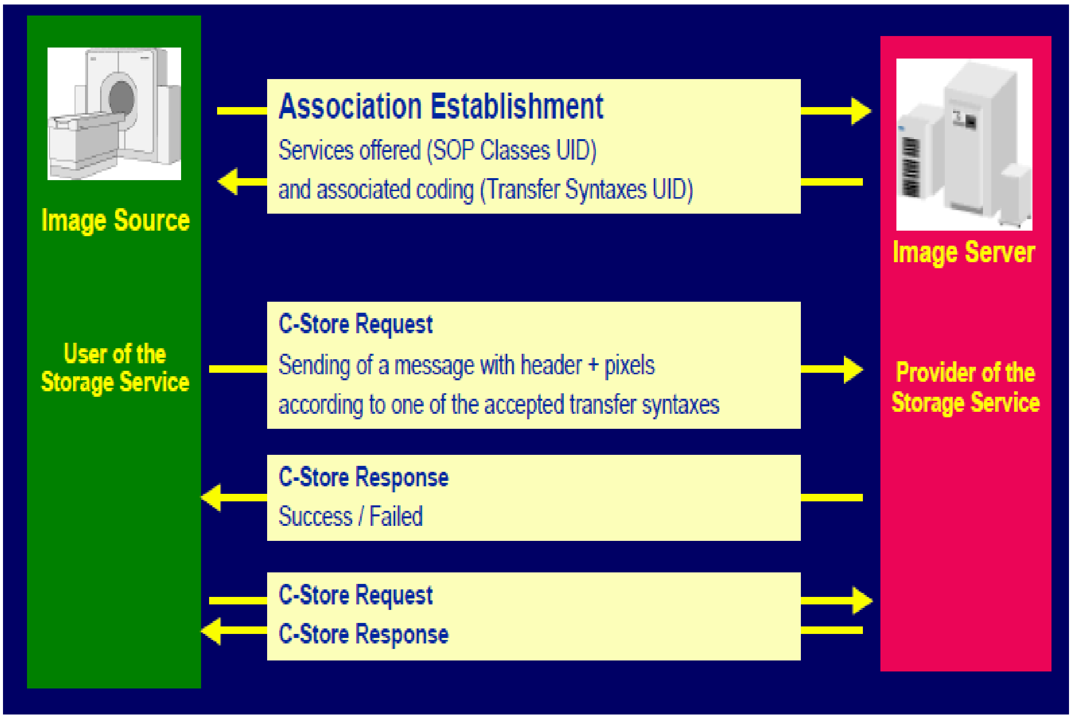


Image Source
User of the Storage Service
Association Establishment
Services offered (SOP Classes UID)
and associated coding (Transfer Syntaxes UID)
C-Store Request
Sending of a message with header + pixels
according to one of the accepted transfer syntaxes
C-Store Response
Success / Failed
C-Store Request
C-Store Response
Image Server
Provider of the Storage Service

3.1.2 Transfer syntax

- ✓ Is an encoding technique used to send data over the network or to write data to a physical media
- ✓ e.g.,
  - VR: Implicit/Explicit
  - Endianism: Little-Endian/BigEndian

3.1.3 Value Representation

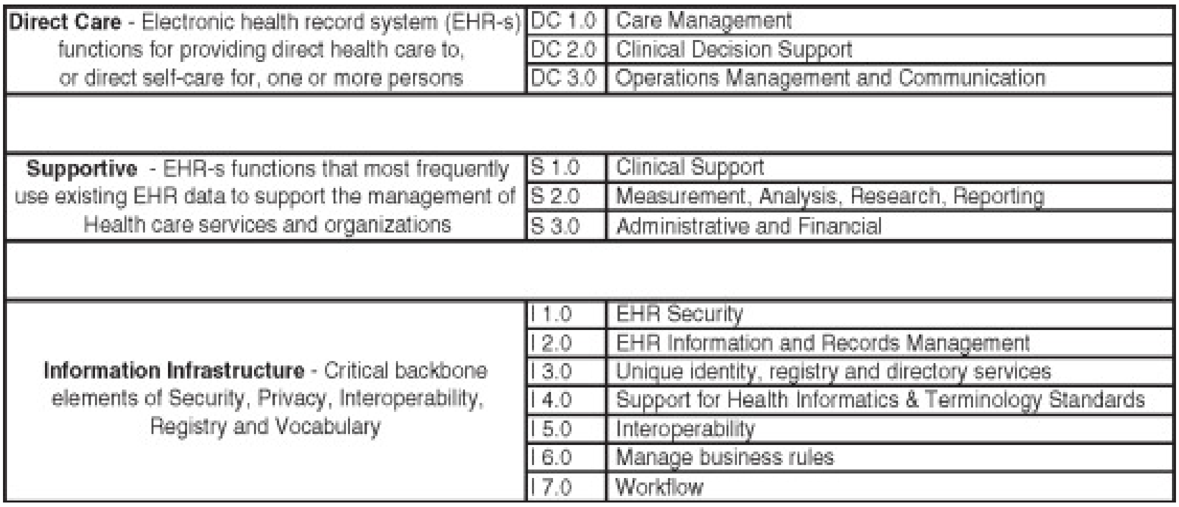
- ✓ Describes the type and the format of the information sent in a DICOM Data Element
- ✓ e.g., The patient Date of birth format is a 8 characters string following the format:YYYYMMDD(19980625)
- ✓ DICOM defines a set of 27 VR's identified with two capital letters
- ✓ E.g., VR codes have to be one of the values from this table

Value Representation	**Description**
AE	Application Entity
AS	Age String
AT	Attribute Tag
CS	Code String
DA	Date
DS	Decimal String
DT	Date/Time
FL	Floating Point Single (4 bytes)
FD	Floating Point Double (8 bytes)
IS	Integer String
LO	Long String
LT	Long Text

Value Representation	**Description**
OB	Other Byte
OF	Other Float
OW	Other Word
PN	Person Name
SH	Short String
SL	Signed Long
SQ	Sequence of Items
SS	Signed Short
ST	Short Text
TM	Time
UI	Unique Identifier
UL	Unsigned Long
UN	Unknown
US	Unsigned Short
UT	Unlimited Text

3.2 HL7(Health Level seven)

- is an ANSI not-for-profit voluntary organization standard for **transfer of clinical and administrative data between software applications used by various healthcare providers.**
- Level seven **focus to the top layer (Application layer) of OSI/ISO**. Therefore it is an Application protocol for Electronic Data Exchange in healthcare Environment
- The seventh layer or the application layer provides **network services to the software (end users). [**remember that normal computer applications are not on this layer, but programs such as browsers, file transfer protocol (FTP) clients, and mail clients are.]
- Developed by **HL7 organization based in Ann Arbor, MI, USA at 1987**.
- Aim is to provide **common "language"** to share clinical data between healthcare applications that is accepted and accredited globally.
- Is a **comprehensive protocol** to transmit **transaction information** (Eg. Patient registration, Insurance, Billing and orders), **Clinical results**(Eg. lab tests, physiological parameters, imaging reports, diet and pharmacy orders).
- Acts as **communication protocol between two independent application** rather than **closely coupled client-server type applications**
- The HL7 functional model consists of a **set of functions and their associated functional descriptors.** These functions are divided into **three main sections: direct care, supportive and information infrastructure**

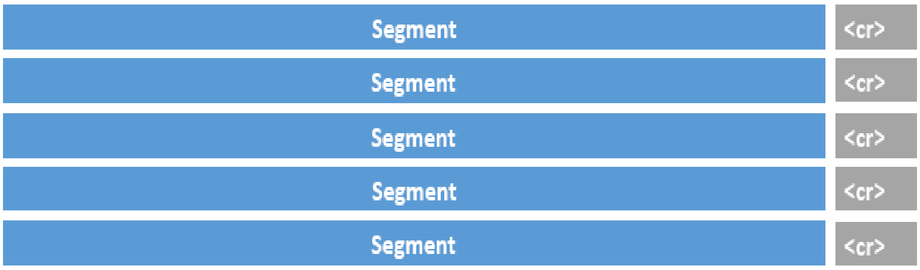


Direct Care - Electronic health record system (EHR-s) functions for providing direct health care to, or direct self-care for, one or more persons	DC 1.0	Care Management
	DC 2.0	Clinical Decision Support
	DC 3.0	Operations Management and Communication
Supportive - EHR-s functions that most frequently use existing EHR data to support the management of Health care services and organizations	S 1.0	Clinical Support
	S 2.0	Measurement, Analysis, Research, Reporting
	S 3.0	Administrative and Financial
Information Infrastructure - Critical backbone elements of Security, Privacy, Interoperability, Registry and Vocabulary	I 1.0	EHR Security
	I 2.0	EHR Information and Records Management
	I 3.0	Unique identity, registry and directory services
	I 4.0	Support for Health Informatics & Terminology Standards
	I 5.0	Interoperability
	I 6.0	Manage business rules
	I 7.0	Workflow

- HL7 protocol comprises of **grammar and vocabulary** that allow clinical data to be shared among the healthcare systems and easily understood by all stakeholders.
- **TCP/IP port or FTP** can be used for exchange data. Most time all HL7 communication between telemedicine systems is done by TCP/IP
- **HL7 Messages**
  - ✓ are used to transfer electronic data between healthcare systems.
  - ✓ Each HL7 message sends information about a particular event (e.g., patient admission).
  - ✓ contents of an HL7 message
    - **component**s of message
    - **delimiter characters** that are used to separate these components
    - HL7 **message type**

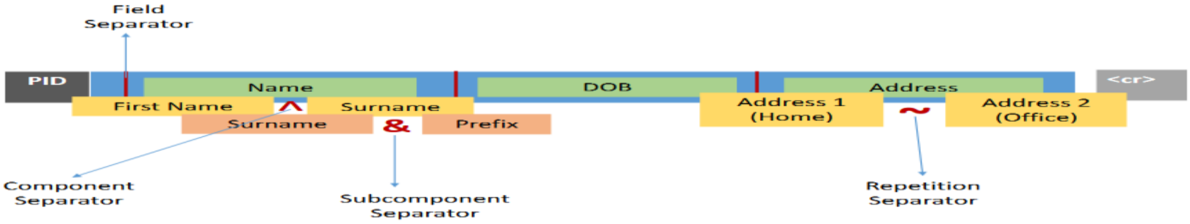
a) HL7 Components

- HL7 messages are in human-readable (ASCII) format.
- Each HL7 message consists of **one or more segments**. A **carriage return character (**\r or<cr>**, which is 0D in hexadecimal) separates one segment** from another. Each segment is displayed on a different line of text. (as seen in the sample HL7 message below)



- Each HL7 segment consists of **one or more composites** (also known as fields). A **pipe** (|) **character is used to separate** one composite from another.

- If a **composite contains other composites**, these sub-composites (or sub-fields) are normally **separated by ^ characters.**
- Example of HL7 Message
  MSH|^~\&|EPIC|EPICADT|SMS|SMSADT|199912271408|CHARRIS|ADT^A04|181
  7457|D|2.5|
  PID||0493575^^^2^ID
  1|454721||DOE^JOHN^^^^|DOE^JOHN^^^^|19480203|M||B|254 MYSTREET
  AVE^^MYTOWN^OH^44123^USA||(216)123-4567|||M|NON|400003403~1129086|
  NK1||ROE^MARIE^^^^|SPO||(216)123-4567||EC|||||||||||||||||||||||||||
  PV1||O|168 ~219~C~PMA^^^^^^^^^||||277^ALLEN
  MYLASTNAME^BONNIE^^^^||||||||||
  ||2688684|||||||||||||||||||||||||199912271408||||||002376853



b) HL7 Segments

- each segment of the message contains one **specific category of information**, such as patient information or patient visit data.
- the **name of each segment** in the message is specified by the **first field** of the segment, which is always **three characters long**.
- The example message contains four HL7 segments: MSH, PID, NK1 and PV1. Different types of HL7 messages contain different HL7 segments.
  - **MSH** (Message Header) segment contains information about the message itself. This information includes the sender and receiver of the message, the type of message this is, and the date and time it was sent. Every HL7 message specifies MSH as its first segment.
  - **PID** (Patient Information) segment contains demographic information about the patient, such as name, patient ID and address.
  - **NK1** (Next of Kin) segment contains contact information for the patient’s next of kin.
  - **PV1** (Patient Visit) segment contains information about the patient’s hospital stay, such as the assigned location and the referring doctor.
  - **SCH((Schedule activity information):** Is for updating appointments in the hospitals schedule.
- Over 120 different HL7 segments are available for use in HL7 messages.

c) HL7 Composites

- Each segment of an HL7 message consists of one or more **composites** (also known as **fields**).
- By default, the **|** (pipe) character is used to separate one composite from another.
- A composite can be a primitive data type (such as a character string or a number), or can contain other composites.
- If a composite contains other composites, these sub-composites (or **sub-fields**) are normally separated by **^** characters.
- If a sub-composite also contains composites, these sub-sub-composites are normally separated by **&** characters. Sub-sub-composites must be primitive data types.

d) HL7 Message Type

- message type defines the **purpose for the message** being sent and is present in every HL7 message
- Message types are identified by a **three-character code**, and are used in **conjunction with a trigger event**
- An HL7 **trigger event** is a real-world event that initiates communication and the sending of a message, and is shown as part of the message type.
- Both the message type and trigger event are found in the **MSH-9 field** of the message.
- For example, consider this MSH segment, which you have seen before:
  - MSH|^~\&|EPIC|EPICADT|SMS|SMSADT|199912271408|CHARRIS|**ADT^A04** |1817457|D|2.5|
  - HL7 message type is **ADT^A04**, **ADT (Admission, Discharge, Transfer)** is the HL7 message type, and **A04 is the trigger event** which is "Register a Patient"/Patient Registration.

➢ **Clinical Document Architecture (CDA) :** an exchange model for clinical documents, based on HL7 Version 3

- ✓ is a **XML-based , electronic standard** developed by HL7 that specifies the **structure and semantics of a clinical document**, such as a billing summary or progress medical note, for the purpose of exchange.
- ✓ It was known earlier as the *Patient Record Architecture (PRA).*
- ✓ is a flexible **standard and is unique since it can be read by the human eye or processed by a machine.**
- ✓ due to its use of XML language, which allows the standard to be broken into two different parts.

    - A **mandatory free-form portion** enables human interpretation of the document, while an **optional structured part** enables electronic processing (like with an EMR system).
    - is an **object-oriented document** that includes text, images and even multimedia can be included in the document.

- ✓ defines a very **generic structure** for delivering "any document" between systems
- ✓ does not specify a **transport mechanism** and can be utilized within a messaging environment or outside of it
- ✓ **six characteristics** Clinical Document Architecture (CDA)
    - ○ **Persistenc**e (remaining in use for a long period)
    - ○ **Stewardship** (maintained by a trusted organization, e.g., a hospital using CDA)
    - ○ **Potential for authentication** (legal attestation that the clinical information is accurate)
    - ○ **Context** (a default context to the record, such as the patient identity and who created the document)
    - ○ **Wholenes**s (the full document, not just parts of it, can be authenticated)
    - ○ **Human readability** (a person can read the material on a browser or mobile device)

- ➢ **CDA Structure**
    - ✓ The XML structure for a CDA document nests data in the followin

Header

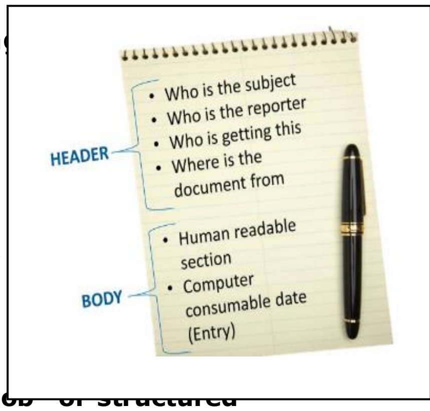
Body

Section(s)

Narrative Block

Entry(s)

1. Header – includes patient information, author, creation date, provider, etc.



2. Body

- ✓ contains the **clinical report and can contain an unstructured "blob" or structured content organizes in one or more Sections.**
- ✓ Each Section contains **one Narrative Block and zero to many coded Entries**

a) Narrative block

- ✓ allows "human-readability" of a CDA document
- ✓ represents content to be rendered for viewing.
- ✓ two ways to populate the CDA Narrative Block: **Directly Authoring. Derivation from Coded Entries**

b) **Entry block**

- ✓ allows "machine readability
- ✓ an entry represents structured content for further computer processing

- HL7 standards are grouped into the following categories

Section 1: Primary standards: for system integrations, inter-operability and compliance.

Section 2: Foundation Standards: defines fundamental tools and building blocks to build the standards and technology infrastructure that implements of HL7 standards must manage

Section 3: Clinical and administrative domains: Messaging and document standards for clinical specialties and groups.

Section 4: EHR profiles: provides functional models and profiles that enable management of electronic health records

Section 5: Implementation guides: is for implantation guides and/or support documents created to be used in conjunction with an existing standard

Section 6: Rules and References - Technical specifications, programming structures and guidelines for software and standards development.

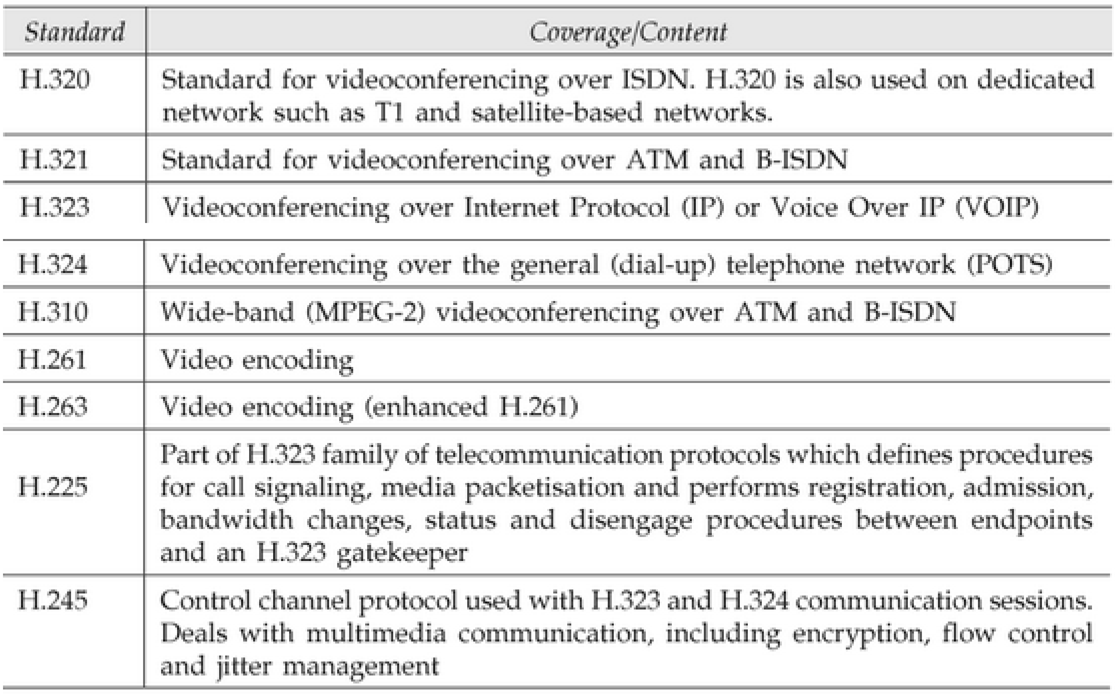
Section 7: Education & Awareness - Find the HL7 Standards for Trial Use (STUs) and current projects here, as well as helpful resources and tools to further supplement understanding and adoption of HL7 standards.

1. **Advantages of Clinical Document Architecture**
   1. is a flexible standard that can be **read by both humans and processed by a machine.**
   2. Makes it possible to **display a patient's entire medical history in one document**.
   3. Can be **reused** in multiple applications.
   4. Aims to eliminate message variability (lack of consistency) that HL7 V2 is prone to.
2. **Challenges of Clinical Document Architecture**
   1. Compatibility: CDA is not backwards compatible with HL7 V2.
   2. Large file size: can easily reach hundreds of millions of lines of XML with file sizes up to 400MB.
   3. Validation: Different customers will have different validation methods, which often won't match the publicly available ones.
   4. Data completion: Having an incomplete set of data can make it difficult to create valid documents.

3.3 H. 320 series Video Conferencing

- Multimedia conferencing/video conferencing is an application of real-time media
- Video conferencing refers to **meeting at a distance that involve combination of audio, video and data collaboration**

- This video conferencing needs some standards to be followed. Two major categories are **a) H.32x series b) SIP(Session initial protocol, based on Internet engineering Task force)**
- H.3xx are "umbrella" ITU recommendations for videoconferencing
- This standard contains **protocols for coding video/audio, multiplexing, signaling and control.**



Standard	*Coverage/Content*
H.320	Standard for videoconferencing over ISDN. H.320 is also used on dedicated network such as T1 and satellite-based networks.
H.321	Standard for videoconferencing over ATM and B-ISDN
H.323	Videoconferencing over Internet Protocol (IP) or Voice Over IP (VOIP)
H.324	Videoconferencing over the general (dial-up) telephone network (POTS)
H.310	Wide-band (MPEG-2) videoconferencing over ATM and B-ISDN
H.261	Video encoding
H.263	Video encoding (enhanced H.261)
H.225	Part of H.323 family of telecommunication protocols which defines procedures for call signaling, media packetisation and performs registration, admission, bandwidth changes, status and disengage procedures between endpoints and an H.323 gatekeeper
H.245	Control channel protocol used with H.323 and H.324 communication sessions. Deals with multimedia communication, including encryption, flow control and jitter management

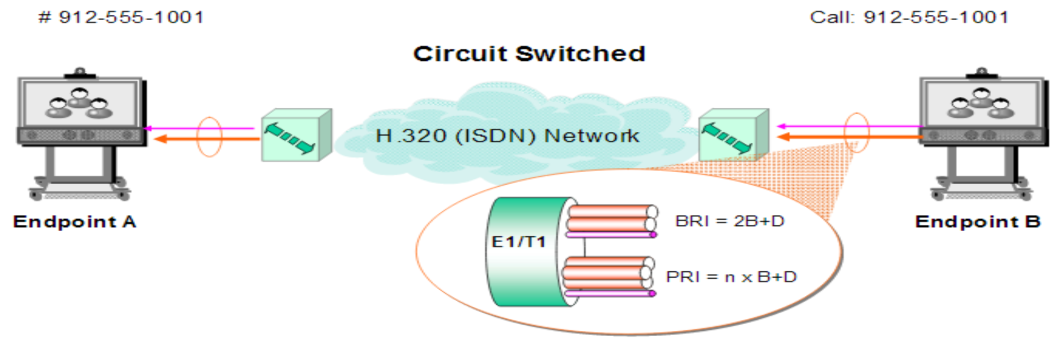
Summary of videoconferencing standards

- Summary of video standards are

3.3.1 H.320(ISDN)/ Narrow-band visual telephone systems and terminal equipment

- is a suite of standards by the ITU-T for **running multimedia (audio/video/data) over ISDN based networks released in the early 1990**
- Defines rules for **establishing communications, framing and synchronizing media and inverse multiplexing ISDN channels**
- The protocol is built to use multiple **ISDN B-channels 64 kbps to send control, audio, video and data information.**

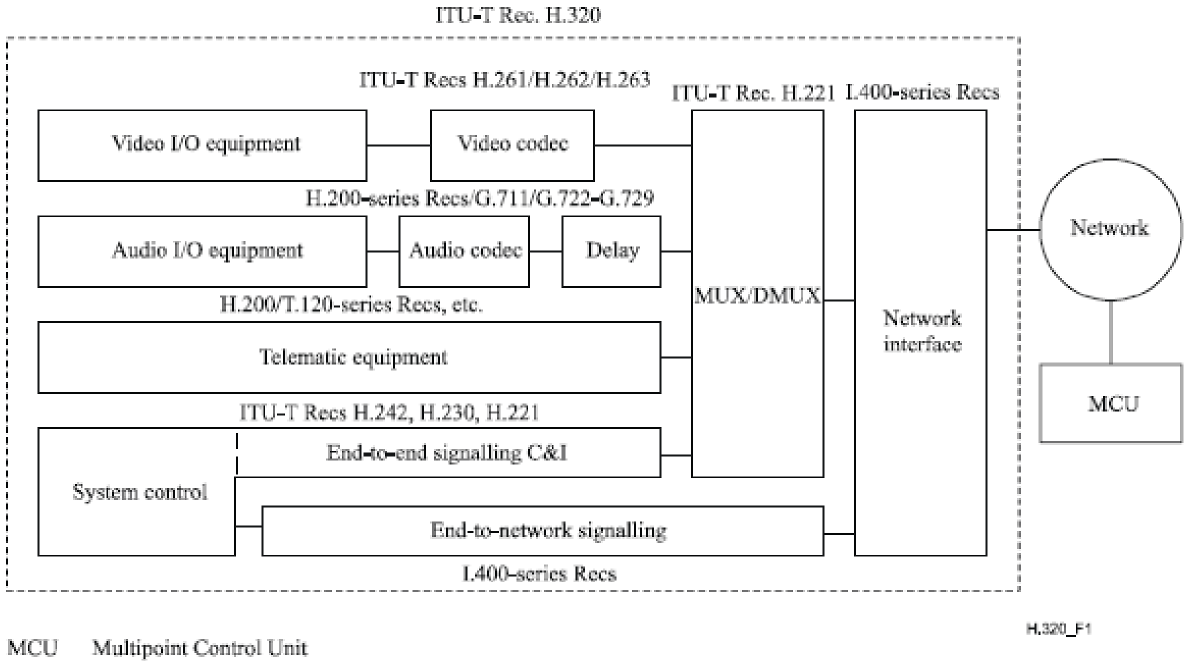
Video Conferencing Protocols: H320



- The main protocols in H.320 suite include the following coding standards

Video	H.261,H.263,H.264
Audio	G.711, G.722, G.722.1, G.728
Data	T.120
Control	H.221,H.231,H.242,H.243

- This standard is adopted by the leading manufacturer of videoconferencing equipment.
- Pictorial representation of H.320 codec for digital video/audio transmission



The H.320 terminal architecture.

– The network interface connects H.221 multiplex protocol with the ISDN port

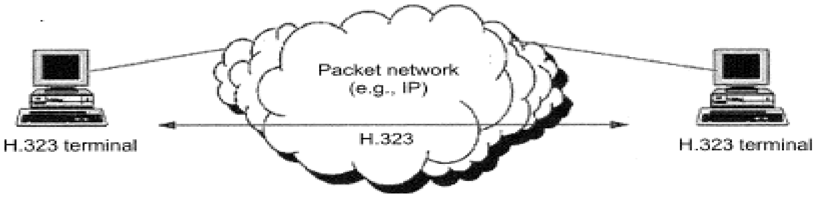
– Together with end-to-end call control module, it servers two purpose

1. D-channel access: used for call control like dialing and supplementary services It is controlled by the End- to-Network signaling module.
2. B-Channel(data channel) access from/to the H.221 multiplexer

- Data is processed by an implementation of H.221 multiplexer/demultiplexer protocol. Two important duties are
  a. To aggregate all connected B-channels (upto 6 simultaneously of 384 kbits/s bit-rate to one combined super-channel)
  b. To split combined super-channel into fractions for the media streams audio/video/data.
  c. Offers so-called service channel for real-time terminal to terminal signaling which is used by the control and signaling protocols H.242 and H.230
- The separated video data is processed by the video codec and audio data is processed by the audio codec.
- Processing of video data takes more latency time than the audio data, a delay unit is necessary to achieve lip synchronization
- Other data is transmitted to the Telematic equipment protocols , which is an implementation of the T.120 protocol series
- The set of four protocols H.320,H.22,H.242,H.230 with conjunction of audio codec(G.711) and video codec(H.261) will form a complete stand alone Videotelephone.

3.3.2 H.323(Internet, LAN)

- is an umbrella standard for multimedia communications over LAN's and Internet
- By complying with H.323, multimedia products and applications from multiple vendors can interoperate, allowing users to communication without concern for compatibility
- Provides multimedia communication over packet networks.
- Pictorial representation of H.323 terminals on a packet network



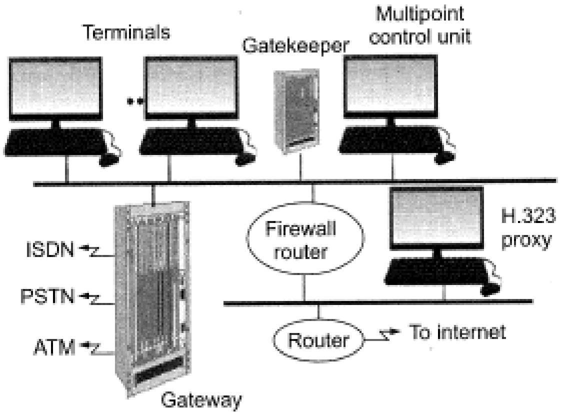
H.323 terminals on a packet network

- H.323 is the ITU standard used for LAN conferencing and Internet conferencing

LAN conferencing	
Video	H.261,H.263,H.264
Audio	G.711, G.722, G.722.1,G.723 G.728,G.729
Data	H.239,T.120
Control	H.225,H.245
Internet conferencing	
Video	H.261,H.263,H.264
Audio	G.723.1,G.722.1,G.728
Data	H.239,T.120

Control	H.225,H.245

- main benefits of H.323 standard is interoperability.
  - Interoperability is achieved through the use of gateway.
  - A gateway performs any network or signaling translation required for interoperability



Function of the gateway in H.323

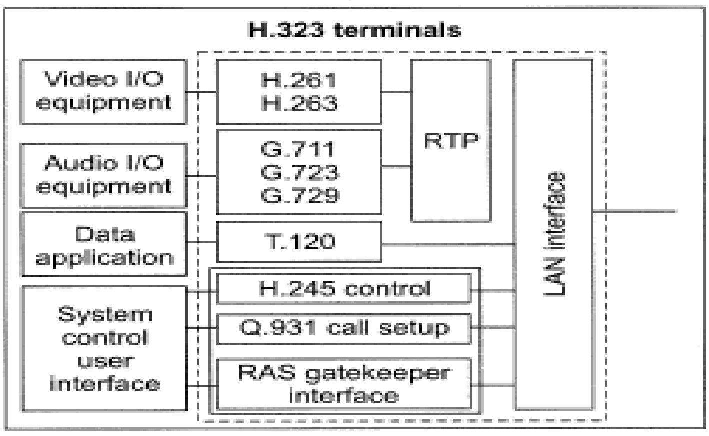
  - H.323 has four optional network components when used with videoconferencing

1. **Terminals**

   An H.323 terminal is an endpoint in the network that provides for real-time, two-way communications with another H.323 terminal, gateway, or multi point control unit (MCU)

2. **H.323 Gatekeepers**
   - Is a entity on the network that provide services such as
     - Address translation (Translating named addresses (such as phone numbers) into IP addresses) and network access control for terminals, gateways and MCUs.
     - Supervises authentication, authorization, call control and routing
     - Bandwidth management: ensuring QoS for voice and video sessions
     - Prevent network congestion by controlling terminal access
   - Are proprietary software products bought from a number of vendors that reside on a servers
   - Gatekeepers are actually optional components, and H.323 networks can operate fine without them. If they exist, however, the above functions are mandatory
3. **H.323 Gateways** : bridge between H.323 and non H.323 devices
4. **Multipoint control units (MCUs):** enable multipoint conferencing. These units contain Multipoint Controllers (MCs) that handle the conference responsibilities – mixing media from multiple sources, switching, etc

- Various components of H.323 standard



3.3.3 H.324(Plain Old Telephone Service)

- suite of standards defining videoconferencing, interoperability over POTS
- establishes low-bandwidth multiplexing/control protocols and includes the following standards

Video	H.263
Audio	G.723
Data	T.120

3.3.4 H.261/H.263/H.264/H.265 standards

1. H.261

- Most widely applied **international video compression standard for video conferencing**
- **first video coding standard** that was useful in practical terms
- H.261 was originally designed for transmission over ISDN lines on which data rates are multiples of 64 kbit/s
- supports two video frame sizes:

  i) Common Intermediate Format(CIF)

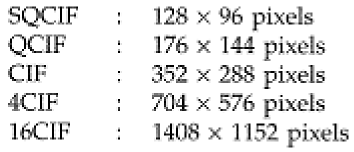
  - Standardized format for the picture resolution, frame rate, color space of digital video sequences used in video teleconferencing systems.
  - Frame size is 352×288 luma (brightness, achromatic image without any color) with 176×144 chroma (colour information

  ii) Quarter Common Intermediate Format(QCIF)

  - a videoconferencing format that specifies data rates of 30 frames per second (fps), with each frame containing 144 lines and 176 pixels per line.
  - This is one fourth the resolution of Full CIF.
  - Frame size is 176×144 with 88×72 chroma

- Block based hybrid compression algorithm to use a combination of discrete cosine transform, DPCM(Differential pulse-code modulation) and motion compensation techniques
- Most of the video coding standards are based on this architecture
- H.261 can support any rate upto 2Mbps connection

2. H.263
   - Originally designed as a **low-bit rate (<64Kbps) compressed format** for videoconferencing.
   - Widely adopted for **video streaming over mobile networks.**
   - Handles **only the visual part of a video stream**. The audio is **encoded using audio encoders.**
   - Can have five resolution modes



SQCIF	:	128 × 96 pixels
QCIF	:	176 × 144 pixels
CIF	:	352 × 288 pixels
4CIF	:	704 × 576 pixels
16CIF	:	1408 × 1152 pixels

   - QCIF image size is consider as the minimum size. Full screen image size is CIF, where the screen size will be 4 times, requires larger computing power

3. H.264/AVC
   - **H.264** is a new video codec standard which can **achieve high quality video in relatively low bitrates**
   - is designed for **enhanced compression performance with network friendly** features such as **conversational(video telephony and video conferencing) and non-conversational(e.g., storage, broadcast and streaming**)
   - Also known as **AVC** (**Advanced Video Coding, MPEG-4 Part 10**), therefore called as H.264/AVC standard.
   - Has the potential to work on **reduced bandwidth to about 50% for digital video services over the internet and 3G wireless networks**
   - Applications are video conferencing, video streaming, mobile devices , telemedicine etc.
   - compression schemes used by Blu-ray(a format of DVD designed for the storage of high-definition video and data)

4. **H.265/HEVC(High Efficiency Video Coding)/ MPEG-H Part 2**
   - is the successor of H.264/AVC
   - Approved by ITU-T in January 2013.
   - In comparison to AVC, HEVC offers from 25% to 50% better data compression at the same level of video quality, or substantially improved video quality at the same rate which effectively lowers infrastructure costs

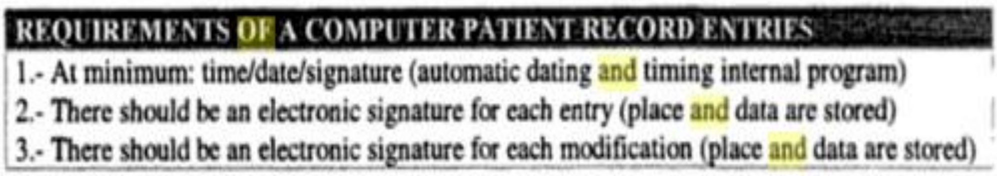
- Handles issues like shortage of bandwidth, spectrum, storage and 4K/UltraHD content of delivery

4. Security and confidentiality of medical records

4.1 Security and legal issues associated with CPR(Computer patient records)

4.1.1. Data Integrity

- Mainly based on i) completeness of the data ii) data maintained by audit trails(a system that traces the detailed transactions relating to any item in an accounting record.)



REQUIREMENTS OF A COMPUTER PATIENT RECORD ENTRIES

1.- At minimum: time/date/signature (automatic dating and timing internal program)

2.- There should be an electronic signature for each entry (place and data are stored)

3.- There should be an electronic signature for each modification (place and data are stored)

Computer patient record entry requirements

4.1.2. Data Security

- is required **to prevent accidental or intentional disclosure** of system security and password
- data security is done by the Information system(IS) department. E.g., backup options

4.1.3. System Security

- To **prevent unauthorized access** through the use of **levels of passwords** , **changed at specified intervals**
- This system will specifically **avoid availability of the information to unintended persons**
    a) Nurses: can see the patient record only on their own unit
    b) Doctors: by level of passwords
- With medical records, **staff must be conscious on their responsibilities for security** and must **report any breaches in security policies**.
- Information system department must have **strict policies**, supported by the highest administrative level with adherence to **penalties for miss using the system.**
- It is strictly enforced to
    - Immediately **removed expired passwords** from personnel
        - Finishing their employment
        - On extended medical leave
    - Assure firewalls systems to avoid external accesses
    - Provide 100% redundancy of data

4.1.4. System reliability

- IS department must assure 100% redundancy and frequent backups
- The staff must
  - Known **how to use the recovery program**
  - Whether **auxiliary power is available for down times**
  - How to **proceed in case of power failure, system failure or disk crash**

4.1.5. Confidentiality

- Confidentiality of data is a **contractual duty** of all health care works, but **IS** department must aggressively prevent unauthorized access
- Three are the legal purposes of documentation, whether in paper or electronic format
  - ➢ To record **assessments throughout an episode**
  - ➢ To assure that **care was planned and given**
  - ➢ That, upon discharge, the patient is ready and have been thought to enable him/her to continue care at home

4.2 Contents in medical records based on NABH(National Accreditation Board for Hospitals & Healthcare Providers) standards

1. Medical record of each patient should have a **unique identification number**.
2. Medical records of currently admitted patients must contain **documented initial assessment within the time-frame** defined by hospital (maximum 24 hours)
3. **Plan of care** should be **signed / counter-signed by consultant** in-charge of the patient
4. If patient is **transferred** to other hospital, medical records should contain **date of transfer, reason of transfer and name of receiving hospital**
5. Each entry in medical records should be **signed, named, dated and timed**
6. **Medication orders and charts** should not have any **non-standard abbreviations**. Or should have only those abbreviations that are defined by the hospital
7. Entries in **medical records should be up-to-date**
8. Follow up **advice, medication and other instructions**
9. **Safety, security and confidentiality of medical records**. Medical records department should additionally take care of following points,
   a. **Sufficient and safe storage** for medical records
   b. Regular **pest control** in medical record storage area
   c. Availability of fire extinguisher near-by and knowledge on how to use the same
   d. Policy of who can access medical records
   e. How to respond to different request for accessing medical records
   f. Mechanism to quickly retrieve the medical records
   g. Screening of medical records

5. Cyber laws related to telemedicine

5.1 Cyber

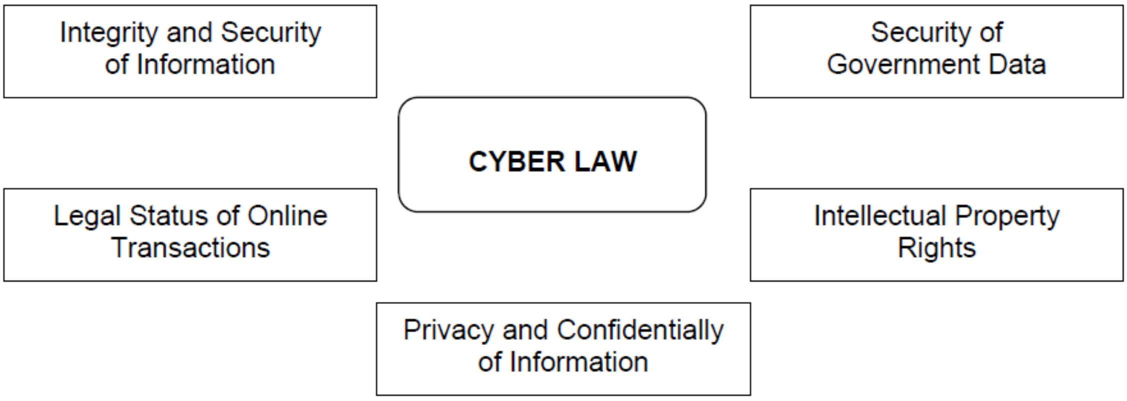
- **Defn-1:** "Cyber" is a prefix used to describe a **person, thing, or idea as part of the computer and information** (computers or computer networks (such as the Internet))
- **Defn-2 (from oxford dictionary):** "Relating to or characteristic of the culture of computers, information technology, and virtual reality."
- taken from *kybernetes*, Greek for "steersman"(a person who is steering a boat or ship.) or "governor,"
- it was first used in ***cybernetics***=> is the science or study of control or regulation mechanisms in human and machine systems, including computers.

5.2 Cyber Crime

- **Defn-1:** is any criminal activity that involves a computer, networked device or a network
- **Defn-2 (from oxford dictionary):** Crime committed over internet
- Types of Cyber crime
  1. Network unauthorized access and penetration
  2. Theft of proprietary information
  3. Financial fraud using computers, internets
  4. Sabotage of data or networks
  5. Disruption of network
  6. Creation and distribution of computer viruses
  7. Software, intellectual property piracy
  8. Identity theft
  9. Terrorism

5.3 Cyber law

- **Defn-1:** refers to any laws **relating to protecting the Internet and other online communication technologies.**
- **Defn-2:** Refers **to all the legal and regulatory aspects** of Internet and WWW.
- **Needs for Cyber Law**


Integrity and Security of Information
Security of Government Data
CYBER LAW
Legal Status of Online Transactions
Intellectual Property Rights
Privacy and Confidentially of Information

- **Why cyber law in telemedicine**

  The practitioners of telemedicine must have **trust in the security of information** and **communications infrastructures, networks and systems in confidentiality, integrity and availability of data on them and in the ability to prove the origin and receipt of data**

5.4 Cyber law in telemedicine

- Defn-1: encompass all the **cases, statutes (act) and constitutional provisions** that impact **persons and institutions** who control the entry to cyberspace, create hardware and software which enable people to access cyberspace.

Statutes of Telemedicine in India

- the practice of Telemedicine in India is governed by Medical Council of India Act, 1956 ("**MCI Act**")
- In MCI Act, a qualified doctor/medical practitioner has registered in any state medical registers must send a copy of his/her registration certificate to Medical Council of India for enrollment in the Indian medical register.
- In terms of Section 27 of the MCI Act, an enrolled doctor in the Indian medical register can practice in any state of India according to his qualifications. Hence, inter-state practice of Telemedicine by medical practitioners is permissible.
- In accordance with the **<u>Drugs and Cosmetic Rules 1945</u>** and **Section 4** of the **<u>Information Technology Act, 2000,</u>** For **all medical treatments through telemedicine or web-interface format**, **the prescriptions issued by the medical practitioner should be in writing and signed by a registered medical practitioner,** without which, the prescription is invalid.
- Telemedicine governed by the **Information Technology Act, 2000**, is to **security, privacy and confidentiality of patient data and potential misuse** and even abuse of electronic records.
- The healthcare service provider adopting telemedicine methods of medical practice must ensure that **medical consultation, prescriptions, treatment and drugs**

are **dispensed only in accordance with legal provisions and guidelines** regulating the medical and healthcare sector in India

Recommended Guidelines & Standards for Practice of Telemedicine in India (by the Department of Information Technology, Ministry of Communications and Information Technology, 2003)

The Guidelines

1. explains the necessary information like introduction to Telemedicine, definitions and concepts, standards required for hardware, software, clinical devices, security aspects and Telemedicine process guidelines.
2. recommend that each healthcare provider(telemedicine consultation centres-TCC, telemedicine speciality centres-TSC) and each patient should have a universal identifier code and Universal patient identifier.
3. recommends hardware and software needed to set up TCC and TSC
4. provide adequate risk mitigation at various stages in the process of Telemedicine.